Notice of Allowability	Application No.	Applicant(s)	
	10/772,065	HOPKINS, W. DALE	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the response of 6/3/2008*.

2. ☒ The allowed claim(s) is/are *1-14,16,17 and 19-30*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date 20080815.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20080815* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Michael J Simitoski/
Primary Examiner, Art Unit 2134

DETAILED ACTION

1. The response of 6/3/2008 was received and considered.

2. Claims 1-14, 16-17 & 19-30 are pending.

Drawings

3. The drawings are objected to because in FIG. 2, STEP 206 should read "COMMUNICATE ENCRYPTED PIN POINT-TO-POINT IN NETWORK". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ken Koestner on 8/15/2008.

The application has been amended as follows:

Please **REPLACE** the **CURRENT CLAIM LISTING** with the **FOLLOWING**:

1. A method for establishing a secure channel through an indeterminate number of nodes in a network comprising:

enrolling a smart card with a unique key per smart card, the unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the ~~secret~~ unique key;

transacting at a point of entry to the network, the transaction creating a PIN encryption key by hashing a keying code that is derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and a transaction sequence number;

communicating a PIN point-to-point in encrypted form through a plurality of nodes in the network; and

recovering the PIN at a card issuer server using the PIN encryption key and the card issuer private key.

2. The method according to claim 1 further comprising:

defining public key values (e, N) that are exclusive to a card issuer system and card base, the key value e being a public exponent and the key value N being a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system;

defining a private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key;

computing a secret key u that is unique to the smart card using an equation of the form:

$$u=x^{d}(\text{mod } N),$$

where x is an entity-identifier that identifies the smart card and the entity; and

storing the secret key u on the smart card with public key values x, e, and N.

3. The method according to claim 1 further comprising:

receiving at an entity-activated terminal an entity-entered Personal Identification Number (PIN) and an entity-inserted smart card;

passing the PIN to the smart card;

computing at the smart card an equation of the form:

$$K=u \cdot TSN^{H}(\text{mod } N),$$

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system; and

hashing at the smart card the keying code K to form the PIN encryption key KPE according to an equation of the form:

KPE=h(K),

where h( ) is a hashing algorithm.

4. The method according to claim 3 further comprising:

hashing at the smart card the keying code K to form an encryption key according to an encryption definition selected from a triple Data Encryption Standard (3-DES) and an Advanced Encryption Standard (AES).

5. The method according to claim 3 further comprising:

padding the keying code K with transaction-related data prior to the hash operation h(K).

6. The method according to claim 3 further comprising:

deriving the PIN encryption key KPE uniquely as a function of the secret key u for each transaction.

7. The method according to claim 6 further comprising:

maintaining the private key value d as a secret known only to the card issuer as the only entity capable of decrypting ~~the cryptogram C~~ a cryptogram C.

8. The method according to claim 1 further comprising:

receiving an encrypted PIN at a card issuer server;

computing a hash H of transaction data;

computing an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t of a transaction sequence identifier TSN that identifies a transaction terminal and a sequence number for a transaction originating at the terminal according to an equation of the form:

$$t=TSN^{e}(\text{mod } N),$$

where N is a modulus in an RSA system;

computing a cryptogram quantity C using public data according to an equation of the form:

$$C=x \cdot t^{H}(\text{mod } N),$$

where x is an entity-identifier that identifies the smart card and the entity;

decrypting the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K=C^{d}(\text{mod } N); \text{ and}$$

decrypting the PIN using a PIN encryption key KPE=h(K) where h( ) is a hashing algorithm.

9. The method according to claim 1 further comprising:

encrypting the PIN at the smart card.

10. The method according to claim 1 further comprising:

receiving at an entity-activated terminal an entity-entered Personal Identification Number (PIN) and an entity-inserted smart card;

passing the PIN to the smart card;

generating a random number r at the smart card that is unique to a transaction;

computing at the smart card an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t according to an equation of the form

$$t=r^{e}(\text{mod } N),$$

where e is the public exponent and N the modulus of the RSA system;

computing at the smart card a hash H of common public transaction data;

computing at the smart card a keying code K and a PIN encryption key KPE according to equations of the form:

$$K=u \cdot r^{H}(\text{mod } N), \text{ and}$$

$$KPE=h(K),$$

where u is a secret key and H is a hash of transaction data elements;

sending the PIN encryption key KPE and RSA system encryption t through the network; and

erasing the random number r.

11. The method according to claim 10 further comprising:

receiving a PIN encryption key KPE and encryption t at a card issuer server;

computing a hash H of transaction data;

computing a cryptogram quantity C using public data according to an equation of the form:

$$C=x \cdot t^{H}(\text{mod } N),$$

where x is an entity-identifier that identifies the smart card and the entity;

decrypting the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K=C^{d}(\text{mod } N); \text{ and}$$

decrypting the PIN using the PIN encryption key KPE=h(K) where h( ) is a hashing algorithm.

12. The method according to claim 1 further comprising:

computing at the smart card a hash H of transaction data;

communicating the transaction data hash to a card issuer server;

computing at the card issuer server a hash of transaction data; and

verifying the communicated hash with the server-computed hash for authentication and integrity checking.

13. A data security apparatus comprising:

a smart card ~~capable of establishing~~ that establishes a secure channel through an indeterminate number of nodes in a network comprising:

an interface ~~capable of~~ for communicating with a card reader and/or writer;

a processor coupled to the interface; and

a memory coupled to the processor that stores a public entity-identifier and a secret unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, the memory further comprising:

a computable readable program code embodied therein that creates a PIN encryption key derived from the smart card unique key and a transaction identifier that uniquely identifies ~~the point~~ a point of entry and transaction sequence number~~.~~;

a computable readable program code causing the processor to receive an entity-entered Personal Identification Number (PIN);

a computable readable program code causing the processor to compute an equation of the form:

$K=u \cdot TSN^{H} (\text{mod } N)$,

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the point of entry and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptogsystem) system; and

a computable readable program code causing the processor to hash the keying code K to form the PIN encryption key KPE according to an equation of the form:

$KPE=h(k)$,

where h() is a hashing algorithm.

14. The apparatus according to claim 13 further comprising:

a secret unique key u stored in the memory with public key values x, e, and N where x is an entity-identifier that identifies the smart card and the entity, key value e is a public exponent and key value N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system, the public key values (e, N) being exclusive to a card issuer system and card base;

wherein the secret key u is unique to the smart card and computed using an equation of the form:

$u=x^{d}(\text{mod } N)$,

where a private key value d is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key.

15. (Canceled).

16. The apparatus according to ~~claim 15~~ Claim 13 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to hash the keying code K to form an encryption key according to an encryption definition selected from a triple Data Encryption Standard (3-DES) and an Advanced Encryption Standard (AES).

17. The apparatus according to Claim 13 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to pad the keying code K with transaction-related data prior to the hash operation h(K).

18. (Canceled).

19. The apparatus according to claim 13 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to hash transaction data elements and communicate the hash point-to-point to a card issuer enabling simultaneous key management and integrity checking.

20. A data security apparatus comprising:

an enrollment system ~~capable of usage for establishing~~ that establishes a secure channel through an indeterminate number of nodes in a network, the enrollment system comprising:

a communication interface ~~capable of~~ for communicating with a writer configured to accept a smart card;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein ~~capable of~~ causing the processor to initialize and personalize ~~a smart~~ the smart card with a unique key per smart card, the unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer~~.~~, the unique key for usage by the smart card to create a PIN encryption key computed by an equation of the form

$$K=u \cdot TSN^{H} (\text{mod } N),$$

where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies a terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, and N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptogsystem) system; and

the smart card hashes the keying code K to form the PIN encryption key KPE according to an equation of the form:

KPE=h(k),

where h() is a hashing algorithm.

21. The apparatus according to claim 20 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to write to an enrolled smart card a stored public entity-identifier and the secret unique key.

22. The apparatus according to claim 20 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to define public key values (e, N) that are exclusive to the card issuer system and card base, the key value e being a public exponent and the key value N being a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system;

a computable readable program code ~~capable of~~ causing the processor to define a private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key;

a computable readable program code ~~capable of~~ causing the processor to compute a secret key u that is unique to the smart card using an equation of the form:

$$u=x^{d}(\text{mod } N),$$

where x is an entity-identifier that identifies the smart card and the entity; and

a computable readable program code ~~capable of~~ causing the processor to store the secret key u on the smart card with public key values x, e, and N.

23. A data security apparatus comprising:

a card issuer server ~~capable of usage for establishing~~ that establishes a secure channel through an indeterminate number of nodes in a network, the card issuer server comprising:

a communication interface ~~capable of~~ for communicating with the network;

a processor coupled to the communication interface; and

a memory coupled to the processor and having a computable readable program code embodied therein ~~capable of~~ causing the processor to recover a Personal Identification Number (PIN) from an encrypted PIN received via the network using a card issuer private key and a transaction PIN encryption key, the transaction PIN encryption key created by hashing a keying code that is derived from a smart card unique key initialized and personalized to the smart card and derived from the card issuer private

key, and a transaction identifier that uniquely identifies a point of entry and a transaction sequence number.

24. The apparatus according to claim 23 wherein:

the smart card unique key is a secret key u that is unique to the smart card and is computed by a card enrollment system using an equation of the form:

$$u=x^{d}(\text{mod } N),$$

where x is an entity-identifier that identifies the smart card and the entity; a private key value d is a secret RSA private key, and key value N is a modulus in an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system, the key values d and N being exclusive to a card issuer system and card base.

25. The apparatus according to claim 23 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to receive a PIN encryption key KPE at a card enrollment server;

a computable readable program code ~~capable of~~ causing the processor to compute a hash H of transaction data;

a computable readable program code ~~capable of~~ causing the processor to compute an RSA (Rivest, Shamir, and Adelman Public Key Cryptosystem) system encryption t of a transaction sequence identifier TSN that identifies a transaction terminal and a sequence number for a transaction originating at the terminal according to an equation of the form:

$$t=TSN^{e}(\text{mod } N),$$

where N is a modulus in an RSA system;

a computable readable program code ~~capable of~~ causing the processor to compute a cryptogram quantity C using public data according to an equation of the form:

$C=x \cdot t^{H} (\text{mod } N)$,

where x is an entity-identifier that identifies the smart card and the entity;

a computable readable program code ~~capable of~~ causing the processor to decrypt the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$K=C^{d} (\text{mod } N)$; and

a computable readable program code ~~capable of~~ causing the processor to decrypt the PIN using the PIN encryption key KPE=h(K) where h( ) is a hashing algorithm.

26. The apparatus according to claim 23 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to receive a PIN encryption key KPE and encryption t;

a computable readable program code ~~capable of~~ causing the processor to compute a hash H of transaction data;

a computable readable program code ~~capable of~~ causing the processor to compute a cryptogram quantity C using public data according to an equation of the form:

$C=x \cdot t^{H} (\text{mod } N)$,

where x is an entity-identifier that identifies the smart card and the entity;

a computable readable program code ~~capable of~~ causing the processor to decrypt the cryptogram quantity C using the private key value d that is exclusive to the card issuer system and card base, the private key value d being a secret RSA private key, the decryption according to an equation of the form:

$$K=C^{d}(\text{mod } N);$$ and

a computable readable program code ~~capable of~~ causing the processor to decrypt the PIN using the PIN encryption key KPE=h(K) where h( ) is a hashing algorithm.

27. The apparatus according to claim 23 wherein the memory further comprises:

a computable readable program code ~~capable of~~ causing the processor to hash transaction data elements and compare the hash to a hash received point-to-point from a smart card enabling simultaneous key management and integrity checking.

28. A transaction system comprising:

a network;

a plurality of servers and/or hosts mutually coupling to the network;

a plurality of terminals coupled to the servers and/or hosts via the network and available for transacting;

a plurality of smart cards enrolled in the transaction system and adapted for insertion into the terminals and transacting via the servers and/or hosts; and

a plurality of processors distributed among the smart cards, the servers and/or hosts, and/or the terminals, at least one of the processors ~~being capable of~~ establishing a secure channel

through an indeterminate number of nodes in the network by communicating, and decrypting a PIN encrypted using a PIN encryption key created by hashing a keying code that is derived from a smart card unique key and a transaction identifier that uniquely identifies a point of entry terminal and a transaction sequence number, the smart card unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer.

29. A transaction system comprising:

a network;

a plurality of servers and/or hosts mutually coupling to the network;

a plurality of terminals coupled to the servers and/or hosts via the network and available for transacting;

a plurality of smart cards enrolled in the transaction system and adapted for insertion into the terminals and transacting via the servers and/or hosts; and

a plurality of processors distributed among the smart cards, the servers and/or hosts, and/or the terminals, at least one of the processors ~~being capable of~~ establishing a secure channel through an indeterminate number of nodes in the network by communicating, and decrypting a PIN encrypted using a PIN encryption key creating by hashing a keying code that is derived from a smart card unique key and a hash of transaction data elements.

30. A transaction system ~~capable of~~ establishing a secure channel through an indeterminate number of nodes in a network comprising:

means for enrolling a smart card with a unique key per smart card, the unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the unique key;

means for transacting at a point of entry to the network, the transaction creating a PIN encryption key by hashing a keying code that is derived from the smart card unique key and a transaction identifier that uniquely identifies the point of entry and a transaction sequence number;

means for communicating a PIN point-to-point in encrypted form through a plurality of nodes in the network; and

means for recovering the PIN at a card issuer server using the PIN encryption key and the card issuer private key.

Allowable Subject Matter

5. The following is an examiner's statement of reasons for allowance:

6. The closest prior art has been discussed in the previous office action.

a. Regarding claims 1, 13, 20, 23 & 28-30, the prior art of record fails to teach or disclose, either alone or in combination, creating a PIN encryption key by hashing a keying code that is derived from a smart card unique key and a transaction identifier that uniquely identifies a point of entry terminal and a transaction sequence number, where the smart card unique key is derived from a private key assigned and distinctive to systems and a card based of a card issuer and encrypting a PIN with the PIN encryption

key, in combination with the other elements of the claims as a whole and as described at least in the specification at ¶20 & ¶22-45.

b. Regarding claim 22-12, 14, 16-17, 19, 21-22 & 24-27, the claims are allowable based on their dependence upon an allowed claim.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

August 15, 2008
/Michael J Simitoski/
Primary Examiner, Art Unit 2134